ASYMMETRISCHE VERSCHLÜSSELUNG

Public-Key Verfahren

Eine Ausarbeitung über die asymmetrische Kryptographie, welche eine kurze Einführung, die Geschichte, das Prinzip, den mathematischen Hintergrund, speziell das RSA-Verfahren und auch die hybride Verschlüsselung beinhaltet.

Lorenz Faber
FTI1 | it.Schule Stuttgart

INHALTSVERZEICHNIS

1 Einführung

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."[1]
– Edward Snowden

Dieses Zitat von Edward Snowden, einem der größten Whistleblower und ehemaligen CIA-Mitarbeiter, beschreibt, wie wichtig es ist, dass Kryptographie stark genug und richtig implementiert sein muss, damit sie wirklich funktioniert und verlässlich ist. Manche Verschlüsselungstechniken standen in der Vergangenheit in der Kritik, jedoch nicht alle Verfahren der Kryptographie wurden als nicht mehr sicher eingestuft. Viele verschiedene asymmetrische Kryptographie-Verfahren gelten noch bis heute als sehr sicher.[2]

Ende der 1970er Jahre wurden die asymmetrischen Verschlüsselungen entwickelt, da es in großen Kommunikationsnetzwerken als sehr aufwendig oder gar unmöglich galt, einen Schlüssel, welcher zur Ver- und Entschlüsselung verwendet wurde, sicher auszutauschen (Symmetrisches Verschlüsselungsverfahren).[3]

Die Frage, warum dennoch auch symmetrische Verschlüsselungsverfahren heutzutage noch verwendet werden, ist berechtigt und kann wie folgt beantwortet werden: „Weil die bekanntesten asymmetrischen Verfahren viel langsamer sind als die besten symmetrischen."[4] Es gibt eine Mischform, die hybride Verschlüsselung, welche die Vorteile aus beiden Verfahren nutzt - dazu aber in einem späteren Kapitel mehr.[5]

2 Geschichte

Das asymmetrische Verschlüsselungsverfahren gibt es vergleichsweise noch nicht so lange und wurde erst 1975 veröffentlicht. Die symmetrische Verschlüsselung hingegen existiert schon seit über 2000 Jahren und kam erstmals zur Zeit des großen Cäsars auf.[6]

Diffie und Hellmann hatten die Idee zur asymmetrischen Verschlüsselung. Ein erstes fertiges Verfahren gab es aber erst 1977, also zwei Jahre später, und wurde von **R**ivest, **S**hamir und **A**dleman konzipiert und veröffentlicht. Dieser Algorithmus, welcher nach den ersten Buchstaben der Erfinder benannt wurde (RSA), wird noch heute oft angewendet. [7] Auch in den Jahren danach kamen immer mehr Verfahren hinzu.

3 Prinzip

Im Vergleich zu dem symmetrischen Verschlüsselungsverfahren werden bei der asymmetrischen Verschlüsselung zwei Schlüssel, ein sogenanntes Schlüsselpaar, anstatt einem Schlüssel verwendet. Der Ablauf ist folgender:

Zuerst wird das Schlüsselpaar generiert, welches einen privaten und einen öffentlichen Schlüssel enthält. Hierbei ist zu erwähnen, dass der private Schlüssel sich nicht aus dem öffentlichen Schlüssel berechnen lassen darf.[8] Der öffentliche Schlüssel wird, wie der Name schon

[1] [1], Absatz 3
[2] Vgl. [1], Absatz 3
[3] Vgl. [2] Kapitel 3.3
[4] [2] Kapitel 3.3, Absatz 2, Zeile 2-3
[5] Vgl. [2], Kapitel 3.3
[6] Vgl. [5], Absatz 2
[7] Vgl. [7], Absatz 2
[8] Vgl. [2], Kapitel 8.1

sagt, veröffentlicht. Dies kann zum Beispiel per direkter Nachricht wie einer Mail oder auch einem Server erfolgen. Bei dieser Vorgehensweise fällt auf, im Vergleich zu der symmetrischen Verschlüsselung, dass dieser Schlüssel nicht über einen sicheren Weg übertragen werden muss und jeder ihn besitzen dürfte. Öfter hofft man auch auf eine globale Verteilung des öffentlichen Schlüssels, damit kein zweiter, gefälschter Schlüssel verbreitet wird.[9]

Wer nun also den öffentlichen Schlüssel hat, kann seine Nachricht an den Empfänger mit diesem verschlüsseln. Die Nachricht kann ausschließlich mit dem geheimen Schlüssel entschlüsselt und angeschaut werden. Der geheime Schlüssel hat nur der Ersteller des öffentlichen Schlüssels und somit der letztendliche Empfänger.

Es ist sehr wichtig, dass der geheime, private Schlüssel nur der Empfänger hat, denn jeder, der diesen Schlüssel hat, kann auch alle Nachrichten entschlüsseln, die von dem anderen mithilfe des öffentlichen Schlüssels verschlüsselt und versendet wurden. [10]

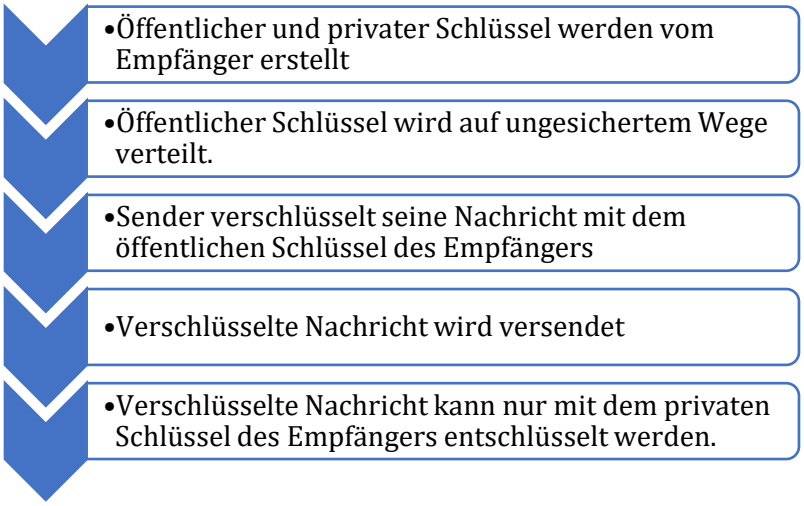

Abbildung 1 Ablauf der Asymmetrischen Verschlüsselung, Lorenz Faber

4 Mathematischer Hintergrund

Der Verschlüsselungsprozess kann auch mathematisch dargestellt werden. Wie schon anfangs erwähnt, werden für die asymmetrische Verschlüsselung ein öffentlicher und ein privater Schlüssel benötigt. Diese hängen zwar mathematisch voneinander ab, doch durch die groß gewählte Länge der Schlüssel ist es praktisch nicht durchführbar den einen von dem anderen zu berechnen. [11]

Ab circa einer Schlüssellänge von 1024 Bit gilt der private Schlüssel nicht mehr mithilfe einer deterministischen Rechenmaschine von dem öffentlichen Schlüssel berechenbar. Diese Länge von mindestens 1024 Bit wird zum Beispiel auch beim RSA-Verfahren verwendet.[12]

In der folgenden Abbildung wird grafisch dargestellt, wie die Asymmetrische Verschlüsselung funktioniert und welche Formeln dahinterstecken. Hierfür steht (e) für den öffentlichen Schlüssel, welcher nicht eingerahmt ist, weil er in keiner geschützten Umgebung ist und (d) für den privaten Schlüssel. Dieser ist umrahmt mit der Ver-/ Entschlüsselungsfunktion (f), weil dieser nur für den letztendlichen Empfänger der verschlüsselten Nachricht zugänglich sein soll. Die Nachricht (m) stellt eine Nachricht in Klartext, aber Binärschreibweise, dar. Die Länge der Nachricht darf die der

[9] Vgl. [5], Absatz 6
[10] Vgl. [5], Absatz 7
[11] Vgl. [6], Kapitel 1.3
[12] Vgl. [6], Kapitel 1.3.3.1

beiden Schlüssel (e, d) nicht überschreiten. Falls die Nachricht länger ist wird sie in einzelne Blocks unterteilt (m_1, m_2, m_3…) somit arbeitet die asymmetrische Verschlüsselung Blockweise.[13]

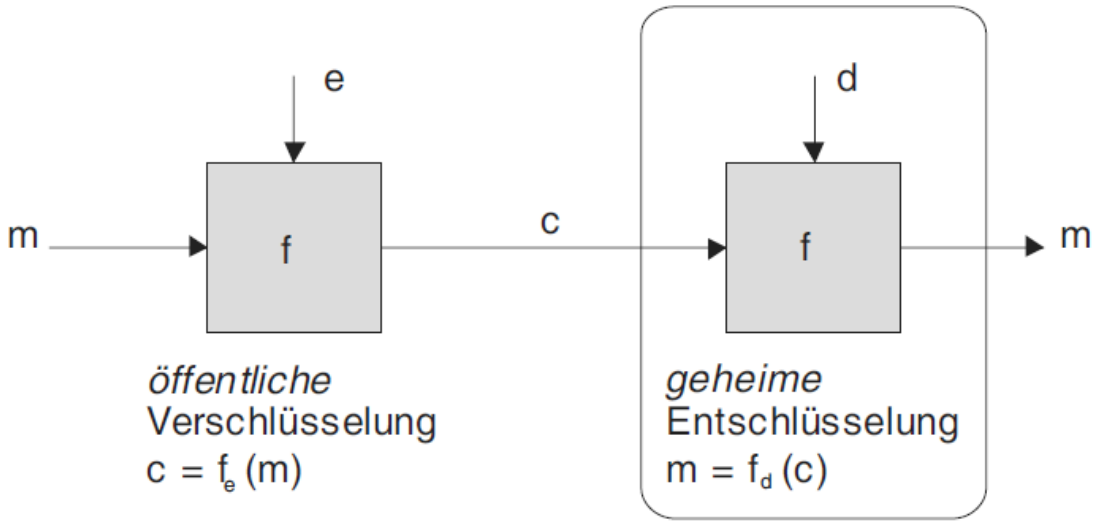

Abbildung 2 Asymmetrischen Verschlüsselung und Entschlüsselung, [6], Absatz 1.3.3.1

Legende:

m: Klartext-Nachricht
c: Verschlüsselte-Nachricht
e: öffentlicher Verschlüsselungs-Schlüssel
d: privater Entschlüsselungs-Schlüssel
f: Verschlüsselungs- und Entschlüsselungsfunktion

5 Das RSA-Verfahren

Wie im Kapitel Geschichte bereits erwähnt, ist das RSA-Verfahren einer der ersten und bis heute bekanntesten Verfahren.[14] Die Sicherheit dieses Verfahrens besteht daraus, große Zahlen in ihre Primfaktoren zu zerlegen. [15]Da dies eine komplexe Vorgehensweise ist, besteht auch darin die Schwierigkeit die RSA-Verschlüsselung zu knacken bzw. zu umgehen. [16]

Das RSA Verfahren beinhaltet folgende Formeln:

$c = m^e \bmod n$ (Verschlüsselung der Nachricht *m* in die verschlüsselte Nachricht *c*)

$m = c^d \bmod n$ (Entschlüsselung der Nachricht *c* in die verschlüsselte Nachricht *m)*

Dabei stehen *c, m, e* & *d* für die gleichen Bestandteile wie bei 4. (*4. Mathematischer Hintergrund)* und *n* ist das Produkt aus zwei beliebigen, ungleichen Primzahlen, welche bezüglich der geforderten Bitstellen (1024 oder 2048 Bit) mehrere hundert Dezimalstellen haben. Wer nun also die Verschlüsselung knacken will muss *n* in seine Primfaktoren zerlegen. Dies ist jedoch durch die Größe der beiden ursprünglich gewählten Primzahlen und somit auch durch die Größe von *n* nicht in einem praktischen Zeitraum lösbar.

[13] Vgl. [6], Kapitel 1.3.3.1
[14] Vgl. [7], Absatz 2
[15] Vgl. [3], Absatz 9
[16] Vgl. [2], Kapitel 8.3

5.1 Gilt es als sicher?

Um zu beweisen, dass das RSA-Verfahren sicher ist muss es praktisch unmöglich sein, den privaten Schlüssel aus dem öffentlichen Schlüssel zu berechnen. Jedoch gilt es als genauso schwer den Divisor (n) des RSA-Moduls in seine Primfaktoren zu zerlegen. Was sagt dies nun? Es kann nicht bewiesen werden, dass RSA sicher ist. Es gilt als sicher, jedoch weiß man nicht, ob es wirklich so ist. Es gibt Argumente dafür, welche behaupten, dass das Faktorisierungsproblem (*hier Primfaktorzerlegung*) seit Jahrhunderten als schwierig gilt, das Berechnen des privaten Schlüssels ist aber genau so schwierig. Somit ist es ein Hinweis dafür, dass es sich als schwierig darstellt, es zu knacken, jedoch lässt es Gegenargumente zu und ist somit kein Beweis, dass es wirklich sicher ist. [17] Seit längerer Zeit ist bekannt, dass Quantencomputer das Faktorisierungsproblem in einer verhältnismäßigen Zeit lösen können, solange diese aber noch nicht wirklich zugänglich sind, gilt das Verfahren als sicher.[18]

Schlussendlich gilt, wenn die Primzahlen richtig gewählt sind und eine sichere Variante von RSA verwendet wird, so ist die einzige bekannte Möglichkeit RSA mit einer deterministischen Rechenmaschine zu brechen das Faktorisieren von *n.* Wie schon erwähnt sind die gewählten Primzahlen so hoch komplex, dass ein klassischer Computer daran scheitert, dies in einer brauchbaren Zeit zu erledigen.[19]

5.2 Anwendungsfälle

Das RSA Verschlüsselungsverfahren wird heutzutage sehr oft und vielseitig angewendet:[20]

- Emailverkehr (PGP oder S/MIME)
- Verschiedene Protokolle (z. B. SSH oder https)
- Digitale Signaturen (zur Authentizitätsprüfung und Verifizierung)
- Chipkarten
- Elektronische Geldgeschäfte

6 Vor und Nachteile der asymmetrischen Verschlüsselung

Vorteile	Nachteile
Die hohe Sicherheit ist ein ganz klarer Vorteil der asymmetrischen Verschlüsselung. Dadurch, dass sehr schwer lösbare mathematische Probleme hinter der Verschlüsselung liegen, kann man diese nicht mithilfe einfacher Angriffe umgehen oder knacken. Außerdem gibt es im Vergleich zu der symmetrischen Verschlüsselung nicht mehr dieses Problem, dass beim Schlüsselaustausch auf einen sicheren Übergabeweg geachtet werden muss. Weil der Öffentliche Schlüssel für jeden zugänglich sein kann, muss dieser nicht geheim ausgetauscht werden. Außerdem werden durch das asymmetrische Verfahren erstmal die Möglichkeiten für	Komplexere Verfahren sind immer rechenintensiver und somit auch langsamer als einfacher konzipierte Verfahren wie es zum Beispiel die symmetrische Verschlüsselung ist. Wie jedoch in dem Kapitel 5.1 aufgeklärt wurde, basiert die Sicherheit der Verfahren nur auf unbewiesenen Annahmen. Sobald ein neuer, besserer und effizienterer Algorithmus auf den Markt kommt, gilt dieses Verfahren als nicht mehr sicher. Außerdem kann ein „Man-in-the-Middle Angriff“ die Sicherheit und somit auch die Übertragung des Verfahrens gefährden, in dem er sich einfach zwischen die zwei Fronten stellt und die Schlüssel vortäuscht ohne, dass

[17] Vgl. [2], Kapitel 8.3.4
[18] Vgl. [4], Absatz 2
[19] Vgl. [9], Absatz 5.7
[20] Vgl. [4], Absatz 10

Authentifikation und digitale Signatur erstellt.[21]	der Sender oder der Empfänger davon mitbekommt, dass ihre komplette Kommunikation abgehört wird. Falls es mehrere Empfänger gibt, muss für jeden Empfänger die Nachricht neu, mit seinem jeweiligen öffentlichen Schlüssel, verschlüsselt werden[22]

7 Hybride Verschlüsselung

Wie schon in der Einleitung erwähnt, gibt es ein hybrides Verschlüsselungsverfahren, welches die Vorteile der asymmetrischen- und der symmetrischen Verschlüsselung nutzt.

Zuallererst wird ein Schlüssel generiert auf Basis des symmetrischen Verschlüsselungsverfahrens, der sogenannte Sitzungsschlüssel. Dieser Sitzungsschlüssel wird mit einem asymmetrischen Verfahren verschlüsselt, heißt, dass der Empfänger dem Sender einen öffentlichen Schlüssel übergibt, mit dem er dann den Sitzungsschlüssel verschlüsseln kann. Im Anschluss wird die Nachricht mit dem Sitzungsschlüssel verschlüsselt und der verschlüsselte Sitzungsschlüssel mit der verschlüsselten Nachricht übergeben. Der Empfänger kann zuerst mit seinem privaten Schlüssel den Sitzungsschlüssel entschlüsseln und anschließen mit diesem die eigentliche Nachricht entschlüsseln.

Vorteil: Das Problem, dass man den Schlüssel der symmetrischen Verschlüsselung nicht geheim übergeben kann existiert nicht mehr und die höhere Geschwindigkeit der symmetrischen Verschlüsselung beim Entschlüsseln der eigentlichen Nachricht wird genutzt.

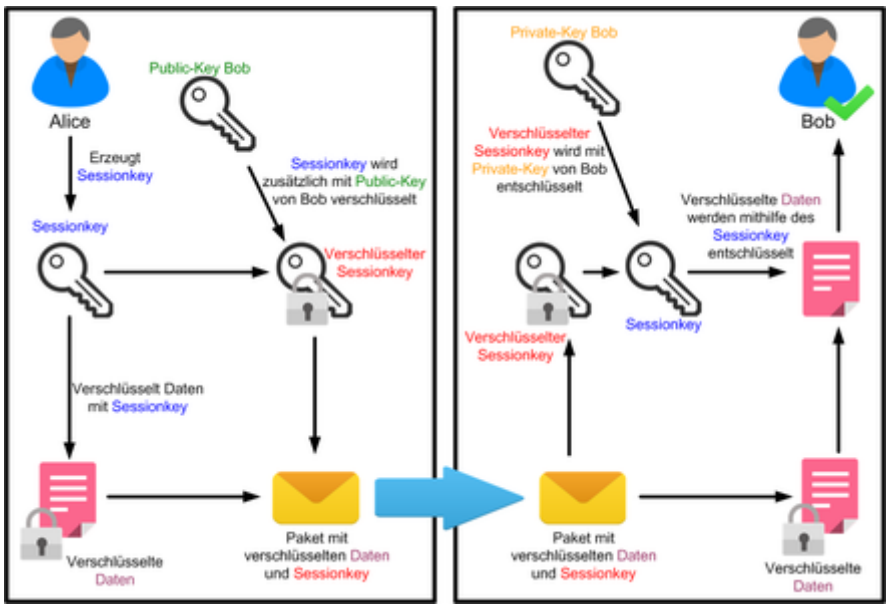

Abbildung 3 Schaubild einer hybride Ver- und Entschlüsselung, [8]

[21] Vgl. [4], Absatz 13
[22] Vgl. [4], Absatz 13

8 ABBILDUNGSVERZEICHNIS

9 LITERATURVERZEICHNIS

[1] ZITATE AUS IT-SICHERHEIT UND HACKING in itsicherheitonline.de, [online] https://itsicherheitonline.de/zitate-aus-it-sicherheit-und-hacking/, [16.01.2021]
[2] Johannes Buchmann: Einführung in die Kryptographie, 6. Auflage Dezember 2015, ISBN 978-3-642-39774-5
[3] Asymmetrische Kryptografie (Verschlüsselung) in elektronik-kompendium.de, [online] https://www.elektronik-kompendium.de/sites/net/1910111.html , [16.01.2021]
[4] Quantenkryptographie in elektronik-kompendium.de, [online] https://www.elektronik-kompendium.de/sites/net/2502221.htm ,[20.01.2021]
[5] Asymmetrische Verschlüsselung in studyflix.de, [online] https://studyflix.de/informatik/asymmetrische-verschlusselung-1609 [18.01.2021]
[6] Asymmetrische Verschlüsselung in kryptowissen.de, [online] https://www.kryptowissen.de/asymmetrische-verschluesselung.html [18.01.2021]
[7] J. Swoboda, S. Spitz, M. Pramateftakis: Kryptographie und IT-Sicherheit Grundlagen und Anwendungen, 1. Auflage 2008, ISBN 978-3-8348-0248-4
[8] RSA Verschlüsselung in sudyflix.de, [online] https://studyflix.de/informatik/rsa-verschlusselung-1608 [18.01.2021]
[9] Datei: Hybride_Verschluesselung.png in commons.wikipedia.org, [online] https://commons.wikimedia.org/wiki/File:Hybride_Verschl%C3%BCsselung.png [20.01.2021]
[10] RSA Verschlüsselung mathematisch erklärt in curi0sity.de, [online] https://curi0sity.de/wissenswertes/rsa-verschluesselung-mathematisch-erklaert/ [20.01.2021]